The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

02/26/2014

SUBJECT:

Multiple Vulnerabilities in Apple QuickTime Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Apple QuickTime that could allow remote code execution. Apple QuickTime Player is used to play media files on Microsoft Windows and Mac OS X operating systems. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, using a vulnerable version of Apple QuickTime Player. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE

At this time there is no known proof-of-concept code available.

SYSTEM AFFECTED:

- Apple QuickTime for Windows 7.7

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple remote code execution vulnerabilities have been discovered in Apple QuickTime that could allow remote code execution. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file. Details of these vulnerabilities are as follows:

- An uninitialized pointer issue exists in the handling of track lists. [CVE-2014-1243]
- A buffer overflow exists in the handling of H.264 encoded movie files**.** [CVE-2014-1244]
- An out of bounds byte swapping issue exists in the handling of QuickTime image descriptions. [CVE-2013-1032]
- A signedness issue exists in the handling of 'stsz' atoms. [CVE-2014-1245]
- A buffer overflow exists in the handling of 'ftab' atoms. [CVE-2014-1246]
- A memory corruption issue exists in the handling of 'dref' atoms. [CVE-2014-1247]
- A buffer overflow exists in the handling of PSD images. [CVE-2014-1249]
- An out of bounds byte swapping issue exists in the handling of 'ttfo' elements. [CVE-2014-1250]
- A buffer overflow exists in the handling of 'clef' atoms. [CVE-2014-1251]

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Apple to affected systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

REFERENCES:

Apple:

http://support.apple.com/kb/HT6151

Security Focus:

http://www.securityfocus.com/bid/65784

http://www.securityfocus.com/bid/65786

http://www.securityfocus.com/bid/65787

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1243

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1244

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1032

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1245

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1246

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1247

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1249

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1250

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1251